University of California
Lawrence Livermore
National Laboratory

Entrust User Agreement

11/30/05

Acknowledgment

I, _____ (print your name), acknowledge I have read and accept the agreement below concerning the use of encryption software on the Livermore Classified Network. Much of this agreement is the same as for Entrust on the unclassified network, but a number of requirements have been added. One of the least expected requirements is that your password and Entrust profile may not be stored in the same repository.

Very Important

You have requested a digital identity (i.e., a digital signature) that is not associated with any particular computer. Like your script signature or fingerprints, it is your unique identifier. Protect it! Your digital signature is made usable via the Entrust software which may be run on several machines at the same time. Unlike fingerprints, when your digital identity is no longer needed, it can be deactivated.

The digital identity enables you to use a digital signature, and allows the encryption of data or text, making it unreadable except to persons you designate. A digital signature is an attachment that is tied mathematically to your data, and of course, as in the real world, only you can create your digital signature. That is, if your digital signature is on the document, you *personally* signed it.

Encryption and digital signatures both require a public and private digital key. The keys are stored on your machine in a password-protected encrypted file. Anyone who has that file *and* your password can sign your name and read your mail; so, protect your password and your machine carefully. Because of a legal concept known as non-repudiation, any document signed with your digital signature is deemed to have been signed by you and you alone; hence, you may be held responsible for documents signed in your name, if your password is shared or stolen. Notify the Entrust PKI team (cln-entrust@llnl.gov) or the LC Hotline (2-4531) immediately if your password becomes known or if your computer is compromised. They can help to protect you if your identity is stolen, and they will issue new keys to you.

Keys are large numbers stored in your machine, and you never see them. The private key gives you access to encrypted files, and allows use of your digital signature. The public key lets other people verify your signature and it lets them encrypt data that only you can read (that is, your public key is needed by others in order for them to interact with you electronically).

Warning -- Notify the Entrust PKI team (cln-entrust@llnl.gov) or LC Hotline (2-4531) immediately if your key is compromised.

You are required to read and abide by the provisions of the US DOE Telecommunications Security Manual, Chapter 9 – Public Key Cryptography and Key Management (https://www.directives.doe.gov/pdfs/doe/doetext/restrict/neword/200/m2001-1ch9.pdf). While many explicit requirements are defined, it is the intent of this document to inform you of the most important of those requirements, and define a model for appropriate procedures and techniques

for using the DOE PKI. Some of the most important issues are summarized below.

Since it is impossible for all practical purposes to break this encryption, it is imperative that your private key not be lost. Your work is a valuable Livermore asset, and your computer files are part of that asset. To insure that Livermore will never lose your files because they cannot be decrypted, your encryption key is automatically archived when it is generated. Keys may be recovered from the archive in three situations, all for the decryption of information, as follows:

1- Key owner access -- Example: You forget your password and want to decrypt a stored file.
2- Non-key owner access excluding law enforcement -- Example: You are not employed at the laboratory any more, and your manager needs access to your encrypted files.
3- Law enforcement access – Example: The FBI wants access to a stored file, and presents appropriate paperwork to the LLNL Legal Department and LLNL ISSM

In addition, Chapter 9 specifies requirements that address the security of the trust relationship between DOE sites. The trust is built on the integrity of all public/private keys in the complex. That trust relationship and everything that supports it is known as the DOE Public Key Infrastructure (PKI). Chapter 9 specifies that any willful acts or gross negligence affecting the viability of any certificate will be viewed as a serious breach (of those requirements). Example: Carelessly allowing someone else to log into Entrust using your password means that people who send you information can no longer be confident that only you have access to the information.

The trust agreement between the various DOE sites is based on a Certificate Policy, CP-1S. The Certificate Policy defines a set of uses for public/private keys and the necessary security for those keys to be trusted by various DOE sites in the defined situations. By accepting a key, you become a party to that agreement. You agree to read and comply with CP-1S, and several important requirements are outlined below. In addition, excerpts from CP-1S are attached to this document for your convenience.

You are required to furnish accurate information in obtaining Entrust. During Entrust initialization, keys are generated and stored on your disk. You are responsible for appropriately protecting the information necessary to initialize Entrust, and for preventing loss of your Entrust identity, disclosure to any other party, modification, or unauthorized use. In case of loss, disclosure or compromise, you are required to notify Entrust PKI team at cln-entrust@llnl.gov or contact LC Hotline at 2-4531. Your Entrust setup is for official use only.

The various DOE sites have agreed on a general level of security needed for the approved applications of public key technology. However, you the user are the final and only authority on whether this particular PKI system is appropriate for your application, and whether you should trust any certificate you receive. The PKI attempts to automate security features, but when it does so, you the end user are the only person who will see a warning if something has gone wrong. It's up to you to educate yourself by reading the various documents, to notice and heed warnings, and to stop the automated processes if appropriate. For example, if someone holding an Entrust certificate turns out to be a bad guy, the PKI administrators can revoke his certificate, but that won't stop you from encrypting information for him or verifying his signature if you ignore the warnings.

Another important scenario is the verification of names. Because of the similarity of peoples' names, the frequent use of nicknames, etc., there is no guarantee that the true identity of the person who owns the certificate will be immediately obvious to you. Be careful, and make some kind of independent check that you have the recipient with the correct need-to-know.

You created your private signature key on your machine and it is not archived. Thus, only you have access to your signature. If the file containing your keys (yourname.epf) is destroyed, your signed and encrypted documents can still be processed using the archive and you can obtain new keys (call LC Hotline at 2-4531 or email the Entrust PKI team at cln-entrust@llnl.gov). Keeping a backup of "yourname.*" from the Entrust directory/folder is reasonable and effective. However, your Entrust password must never be stored in the same repository as the private key (or token containing the key). All this information, for systems on the secure network, is Secret Restricted Data and must be protected accordingly. When your Entrust profile is no longer needed, it must be destroyed. In addition, you must be sure that your Entrust software can't be accessed when you are away from your machine.

Using Entrust -- important information on proper use
The person encrypting a document is always able to decrypt it (unless it is corrupted).

From a security viewpoint, encrypting protects the privacy and integrity of the data. Just signing the file adds your digital signature and protects data integrity but does nothing for privacy. The option "encrypt and sign" takes very little more time, and we recommend using it to avoid confusion.

Compression of encrypted files is not likely to be very successful and you may corrupt a file. However, an Entrust option will automatically compress files for you before encryption and un-compress transparently after decryption.

Encryption provides solid protection for unclassified data (UCI). It is not Type 1 encryption, and thus is not approved to protect classified information from disclosure. However, you may use it on an APPROVED classified network to provide additional protection that helps assure you that nobody but the recipient can see the information you send out.

- Clarification of rules for transmission of Sigma 15 via SecureNet inter-site
  - **Secret (S) Sigma 15 can be sent via SecureNet inter-site, but must be encrypted**
  - Top Secret (TS) Sigma 15 cannot be sent inter-site via SecureNet
  - S/TS Sigma 14 cannot be sent inter-site via SecureNet

- Clarification of rules for transmission of Sigma 15 via SecureNet intra-site
  - Secret (S) Sigma 15 can be sent via SecureNet intra-site w/o encryption, as long as it remains within the site firewall
  - TS Sigma 15 cannot be sent intra-site via SecureNet
  - S/TS Sigma 14 cannot be sent intra-site via SecureNet

If the user chooses to backup their private key to removable media, they must first adhere to the Classified Removable Electronic Media (CREM) policy established within their Directorate. If the

user also chooses to save the pin or password used to unlock the private key it must be stored in a sealed envelope with the user's signature across the seal. The pin or password must never be stored in the same location as the private key.

Required option

Before using Entrust, select the Entrust options menu and set the encryption option to use Triple DES. This is a DOE requirement.

University of California
Lawrence Livermore
National Laboratory

Your signature is required to be witnessed by the Entrust PKI Team Registration Authority (RA). Please sign below upon receiving form "Acknowledge of Receipt of Entrust Keys and Acceptance of Responsibilities" from the RA located in the LC Hotline.

Print Name	Signature	Date
Employee Number	OUN	
RA Witness Name	RA Witness Signature	Date
RA Employee Number	RA OUN	

University of California
Lawrence Livermore
National Laboratory

Excerpts from CP-1S

In this attachment, your role is that of the "subscriber" or "End Entity". The "CA" refers to the Certification Authority, represented at Livermore by the Entrust Administrator, and the framers of computer security policy.

2.2.3.1 Accuracy of Representations

The subscriber certifies that all representations made by the subscriber to the sponsor, CA, or RA regarding the information in the certificate are true.

2.2.3.2 Protection of End Entity Private Keys

The subscriber shall retain control of the subscriber's private keys and key materials, and protect them in accordance with section **Error! Reference source not found.** of this Policy. The subscriber shall take necessary precautions to prevent loss, disclosure to any other party, modification, or unauthorized use. The subscriber shall likewise protect activation data, except that activation data intended for one-time use shall be securely disposed of after use.

2.2.3.3 Restrictions on End Entity Private Key Use

Private keys are issued for the exclusive use of the End Entity in the conduct of DOE business, as stated in section 2.1.

2.2.3.4 Notification of Loss, Disclosure, or Compromise

The subscriber shall notify the CA or RA immediately upon any actual or suspected loss, disclosure, or compromise of the subscriber's private keys or activation data.

2.2.3.5 Decryption Key Recovery

The subscriber understands that the CA maintains the ability to recover the subscriber's private decryption key. The CA may, as required by law or authorized DOE officials, or under other circumstances specified in the applicable CPS, recover the subscriber's private decryption key and decrypt any data encrypted with the corresponding public key.

2.2.5 Relying Party

A relying party is any recipient of a certificate who acts in reliance on that certificate.

Certificate users and relying parties must assure themselves, by reviewing the Certificate Policy (CP-1S), the Certificate Practice Statement (CPS), and any other information they deem necessary, that any certificate issued or other service provided by a CA under this Policy is suitable for the intended use.

This responsibility includes, but is not limited to, stipulations in sections Error! Reference source not found. **through** Error! Reference source not found.**. Actions to provide such assurance are at the discretion of the relying party; however, failure to adequately consider these factors does**

not relieve the relying party of this responsibility.

2.2.5.1 Reading and Understanding This Policy and Supporting CPS

This Policy and supporting CPS contain information that is essential to understanding the limitations of usage and trustworthiness of certificates and other services provided by the subject CA. It is the responsibility of the relying party to read and understand this Policy and the supporting CPS. In cases where intersite agreements exist, it is the responsibility of the relying party to read and understand such agreements before relying on certificates from other sites.

2.2.5.2 Assurance That Certificates Are Issued Under This Policy

It is the responsibility of the relying party to inspect the policy extension field in each received certificate (if the CA supports the policy extension field), or to otherwise assure him or herself that the certificate has been issued under this Policy.

2.2.5.3 Verification of Certificates

It is the responsibility of the relying party to verify the CA signature on received certificates and CRLs, and to insure that a valid certification path is used for verification.

2.2.5.4 Revocation/Suspension Check

It is the responsibility of the relying party to check for certificate revocation or suspension prior to using a certificate.

2.2.5.5 Resolution of Uncertainties in Subject Names

When a CA issues a certificate, the CA insures that the subject of the certificate presents adequate proof of identity, as specified in this Policy and the CPS, at the time of certificate issuance. Likewise, the CA certifies that the subject's distinguished name is unambiguous within the domain of the CA.

Because of the similarity of peoples' names, the frequent use of nicknames, etc., this does not necessarily insure that the true identity of the subject will be immediately and unambiguously obvious to the relying party.

It is the responsibility, therefore, of the relying party to resolve to his or her satisfaction that the distinguished name and other identifying information in the certificate corresponds to the intended subject. This includes resolving any confusion or ambiguity in surnames, given names, host computer names, e-mail addresses, organizational affiliations, etc.

2.5.1 Normal Operation

In normal operation, CAs shall not have access to the private keys of entities they certify. RAs and end entities shall not have access to the private keys of any other end entity. The previous statement is not intended to exclude an individual from being the subject of more than one entity certificate, in which case that individual would have access to the private keys for each of those entities.

2.5.2 Exceptions for Encrypted Data Recovery

Exceptions to section 2.5.1 shall be made for cases in which the CAs and/or RAs must have access to the private decryption keys of the entities they certify or support for the purpose recovering encrypted data as specified in Section **Error! Reference source not found.**. These keys shall be protected in accordance with technical security provisions in Section 6, and shall not be disclosed to any other party without the prior consent of the subscriber or authorized agents, or as required by law. The procedures and conditions under which private decryption key disclosure is authorized shall be specified in the CPS.

2.5.3 Exceptions for Conveying Private Keys to End Entities

Exceptions to section 2.5.1 may be made for cases in which it is impossible or impractical to have the end entity generate their own signing private keys as mandated in section 6.1.1. In such cases, the CA or authorized CA representative may generate the end entity signing private keys and other key material and convey them to the end entity. These keys shall be protected in accordance with technical security provisions in Section 6 and not disclosed to any other party.

The CA shall document all such exceptions for each occurrence. The conditions under which this process may be utilized, and the requirements for authorization, secure generation, and secure conveyance, shall be fully specified in the applicable CPS.

2.5.4 Exceptions for Diagnosing and Troubleshooting Problems

Exceptions to section 2.5.1 may be made for cases in which it is impossible or impractical for a CA or RA to troubleshoot, diagnose, or repair system or user problems without access to the private keys of an end entity. In such cases, the entity may disclose their private keys or activation data to the CA or authorized CA representative. These keys shall be protected in accordance with technical security provisions in Section 6 and not disclosed to any other party.

In all such cases, the end entity shall give informed, signed consent to the disclosure of their private keys or activation data. As soon as the problem is resolved, the CA shall take immediate measures to resume secure operation (such as revoking and re-issuing end entity certificates, requiring the end entity to change the activation data, etc.).

The CA shall document all such exceptions for each occurrence, to include the signed statement of the subject entity. The conditions under which this process may be utilized, and the requirements for authorization and continuity of secure operation, shall be fully specified in the applicable CPS.

5.1.3 Physical Security Controls for End entities

End entity private keys, activation data, and hardware tokens (if used) shall be protected in accordance with DOE or site policies for protection of like information in the classified environment (e.g., Kerberos passwords for SecureNet). The CPS shall specify the protection mechanism or refer to other DOE or site policies for protection of such information.

End entity private keys may be stored in encrypted form on a diskette, computer hard drive, or other medium, provided that:

- The medium is approved for use on the user's end entity workstation in the classified environment and is appropriately marked for classification level, and
- The private key information is encrypted with an approved encryption algorithm, protected by the subject's password or passphrase.

The PIN or password used to unlock the private key protection or hardware cryptographic token shall never be stored in the same location as the private key or token itself.

Preferably, PINs, passwords, etc., should be memorized and not written down. If a PIN or password must be written down, it shall be protected as above. The CPS may specify certain emergency roles and conditions for storage, retrieval, and handling of this information by other persons. The CA shall document the use of such emergency procedures for each occurrence.

End entities shall not leave their workstations unattended when the cryptography is in an unlocked state such that it could be utilized by an unintended party.

6.2.3 Method of Deactivating and Destroying Private Key

Upon termination of use of a private signing key or private decryption key, all copies of the private key shall be securely destroyed.